Over IP-adressen en persoonsgegevens, en het verschil tussen individualiseren en identificeren

G-J. Zwenne[*]

1.Inleiding

De tekst die u nu leest is geschreven op een netbook-computer die op enig moment via door KLM-AirFrance en Starbucks aangeboden WiFi-diensten verbonden was met internet. Een van de IP-adressen waarvan gebruik werd gemaakt was 194.209.131.192. Is dit nummer een persoonsgegeven? Is het mogelijk dat ik, of misschien iemand anders, aan de hand van dit 12-cijferig nummer, al dan niet in combinatie met andere beschikbare gegevens en zonder onevenredige inspanning, kan worden geïdentificeerd?

Ik denk van niet. Voor zover ik weet maakten telkens vijftig tot zestig personen gebruik van de draadloze internetverbindingen en geen van hen heeft voor het gebruik daarvan identificerende gegevens opgegeven. Zo gaat dat op vliegvelden en bij koffiebars, zoals ook in internetcafés, hamburgerrestaurants, openbare bibliotheken enzovoorts. Het is onmogelijk, althans zou een onevenredige inspanning vragen, om te achterhalen wat de identiteit is van al deze internetgebruikers. En dat betekent dat de gebruikte IP-adressen geen persoonsgegevens zijn en dat dus is de Wet bescherming persoonsgegevens (Wbp) niet daarop van toepassing is.

Niet iedereen denkt er zo over. In Nederland en in Europa stellen privacytoezichthouders zich meer en meer op het standpunt dat IP-adressen eigenlijk altijd als persoonsgegevens moeten worden aangemerkt of in elk geval als zodanig moeten worden behandeld. De redenen waarom lijken verband te houden met steeds intelligenter wordende zoek- en profileringstechnologieën en de implicaties daarvan in termen van privacy. In het licht daarvan kan er, zo lijkt de redenering van de toezichthouders te zijn, beter teveel dan te weinig onder de werkingssfeer van de privacywet worden gebracht.

In deze bijdrage, die het eerste deel betreft van een tweeluik over de regulering van IP-adressen,[1] ga ik in op deze ontwikkeling. Ik begin met een korte uiteenzetting van wat de wetgevers heeft gezegd over het begrip persoonsgegevens en geef een overzicht van hoe privacytoezichthouders daarover de afgelopen jaren zijn gaan denken. Vervolgens bespreek ik een en ander en speculeer ik over de redenen achter de ontwikkeling van hun opvattingen. Ik kom tot de conclusie dat de toezichthouders ten onrechte de begrippen 'individualiseren' en 'identificeren' verwarren en aldus de reikwijdte en toepassing van de Wet bescherming persoonsgegevens (hierna: Wbp) op oneigenlijke wijze oprekken.

In het tweede deel van dit tweeluik, dat in een van de volgende nummers van dit tijdschrift wordt opgenomen, bespreek ik waarom regulering van IP-adressen en vergelijkbare nummers nodig kan zijn en hoe een dergelijke regulering kan worden vormgegeven.

2. Persoonsgegevens in de privacyrichtlijn en -wet

Voor de toepassing van de Wet bescherming persoonsgegevens is het begrip 'persoonsgegevens' beslissend. Art. 2, onder a, van privacyrichtlijn 95/46/EG definieert het begrip op de volgende wijze:

> 'persoonsgeven: iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'

In dezelfde bepaling wordt toegelicht wat moet worden verstaan onder 'identificeerbaarheid':

> 'als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit'

Elders in de richtlijn wordt uitgelegd op welke wijze moet worden vastgesteld of iemand kan worden geïdentificeerd. Er moet, zo blijkt uit de preambule[2] worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke, dan wel door enig

---

* Gerrit-Jan Zwenne is, behalve redacteur van dit tijdschrift, advocaat bij Bird & Bird te Den Haag en universitair hoofddocent bij eLaw@Leiden, centrum voor recht in de informatiemaatschappij, van de Universiteit Leiden. Deze bijdrage is voor een belangrijk deel, maar niet volledig, gebaseerd op een bijdrage in L. Mommers e.a. (red.), *Het Binnenste Buiten*, liber amicorum Aernout H.J.Schmidt, Leiden 2010.

1. Onder verwijzing naar RFP760 (January 1980) wordt een 'internet address (IP-address) wel omschreven als 'a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.'
2. Overw. 26.

ander persoon, in te zetten zijn om een natuurlijke persoon te identificeren. Er is derhalve geen sprake van persoonsgegevens als het gaat om:

> '…gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is.'

De Wbp heeft minder woorden nodig om hetzelfde te zeggen. Art. 1, onder a, van de wet stelt dat onder een persoonsgegeven wordt verstaan:

> 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.'

Ook in de parlementaire geschiedenis wordt ingegaan op het identificeerbaarheidscriterium. In ongeveer dezelfde bewoordingen als de richtlijn wordt toegelicht dat moet worden uitgegaan van alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke dan wel enig ander persoon zijn in te zetten om die persoon te identificeren. Het uitgangspunt is dat van 'een redelijk toegeruste verantwoordelijke'. Onder verwijzing naar eerdere uitingen van de privacytoezichthouder[3] wordt opgemerkt dat er:

> '[i]n concrete gevallen rekening [moet] worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke. Het gaat dus enerzijds om objectivering naar een redelijk toegeruste verantwoordelijke en anderzijds om subjectivering naar bijzondere expertise […]. Een onderzoeksinstituut als het CBS zal bijvoorbeeld gelet op zijn expertise, contacten en technische outillage, eerder in staat zijn gegevens te identificeren dan een individuele onderzoeker. Deze omstandigheid dient in de beoordeling of sprake is van een persoonsgegeven te worden meegewogen.' [4]

Voor de vraag of een IP-adres heeft te gelden als persoonsgegeven, en als zodanig onder de werking van de Wbp valt, is derhalve bepalend in hoeverre het mogelijk is om aan de hand daarvan iemand te identificeren. Het gaat erom in hoeverre degene die over het gegeven beschikt in staat is daarmee de identiteit van de desbetreffende internetgebruiker te achterhalen. En daarbij gaat het niet om een zuiver theoretische of hypothetische maar reële mogelijkheid dat de verantwoordelijke of iemand anders aan de hand van het IP-adres en met de hem redelijkerwijs beschikbare middelen ('expertise', 'contacten', 'technische outillage', enz.) in staat is deze identiteit te achterhalen.
Een en ander impliceert dat een gegeven mogelijk ten opzichte van de éne wel als persoonsgegeven wordt aangemerkt en tegelijkertijd tegenover een ander niet - dat is als de eerstgenoemde wel en de laatstgenoemde niet over de mogelijkheden beschikt om de identiteit van de betrokkene te weten te komen.

3. toezichthouders over IP-adressen

Zowel deArt. 29 Werkgroep, het Europees overlegorgaan van privacytoezichthouders, als het College Bescherming Persoonsgegevens, onze eigen nationale toezichthouder, hebben zich de afgelopen jaren verschillende keren uitgelaten over IP-adressen. Uit een handvol werkdocumenten, opinies, oordelen, richtsnoeren (en dergelijke) kan worden opgemaakt dat hun opvattingen een ontwikkeling doormaken. Waar de toezichthouders eerst nog nadrukkelijk onderkenden dat IP-adressen niet altijd kunnen worden aangemerkt als persoonsgegevens, zijn zij de laatste jaren het standpunt gaan innemen dat IP-adressen eigenlijk altijd als persoonsgegevens moeten worden aangemerkt of in elk geval altijd als zodanig moeten worden behandeld.
Ik geef een overzicht te geven van verschillende uitingen van de werkgroep en het CBP.

3.1 'IP-adressen zijn niet altijd persoonsgegevens' (1999 tot 2007)

Eind vorige eeuw komt de Art. 29 Werkgroep met een verkennend werkdocument over verwerkingen van persoonsgegevens op internet. Daarin merkt de werkgroep op dat 'bepaalde' internetprotocol-adressen persoonsgegevens kunnen zijn. De werkgroep onderkent daarmee dat dit niet altijd voor alle IP-adressen heeft te gelden.[5]
Zo een anderhalf jaar later werkt de werkgroep dit uit. In een werkdocument over internet en online-gegevensbescherming komt de werkgroep tot de conclusie dat in elk geval de door een ISP uitgegeven IP-adressen voor deze ISP hebben te gelden als persoonsgegevens. Dit omdat (of eigenlijk: voorzover) kan worden aangenomen dat deze internetaanbieder systematisch de datum, het tijdstip, de duur en het aan hun gebruikers verstrekte IP-adressen vastlegt. Volgens de werkgroep brengt dit met zich mee dat:

> 'internetaanbieders en beheerders van lokale netwerken [kunnen] zonder veel moeite internetgebruikers [kunnen] identificeren aan wie ze IP-adressen hebben verstrekt, doordat ze als regel systematisch de datum, het tijdstip, de duur en het verstrekte dynamische IP-adres van gebruikers in een logbestand vastleggen. [..] In deze gevallen is het buiten kijf dat men kan spreken van persoonsgegevens.'[6]

De werkgroep tekent daarbij wel aan dat dit voor anderen dan de ISP anders kan zijn, omdat zij niet vanzelfsprekend in staat zijn om met IP-adressen internetgebruikers te identificeren. Daarbij maakt de werkgroep onderscheid tussen enerzijds vaste of statische IP-adressen waarmee identificatie geacht wordt eenvoudiger te zijn, en anderzijds dynamische IP-adressen waarbij dat moeilijker is:

> 'Anders is het als derden wel het dynamische IP-adres van een gebruiker kunnen achterhalen, maar dat niet kunnen koppelen aan andere gegevens die identificatie van de betrokken gebruiker mogelijk maken. Identificatie van internetgebruikers die een statisch IP-adres toepassen, is uiteraard eenvoudiger.'[7]

---

3. Vgl. Registratiekamer 27 maart 1995, (kenm. 95.V.029).
4. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48-49.
5. Art. 29 WG, Processing of Personal Data on the Internet, 23 February 1999 < http://bit.ly/TvIR_Art29WGno16>.
6. Art. 29 WG, Een geïntegreerde EU-aanpak van on-line-gegevensbescherming, 21 november 2000 < http://bit.ly/TvIR_Art29WGno37>, p. 22.
7. Art. 29 WG, Een geïntegreerde EU-aanpak van on-line-gegevensbescherming, 21 november 2000 < http://bit.ly/TvIR_Art29WGno37>, p. 22.

Daaraan voegt de werkgroep echter toe dat het toch in voorkomende gevallen wel mogelijk zal zijn om degenen die van IP-adressen gebruik maken te identificeren, en wel door het vaste of dynamische IP-adres te koppelen aan andere gegevens die over de gebruiker zijn verkregen, bijvoorbeeld via cookies of datamining. Om deze redenen gaat de werkgroep ervan uit dat veel, maar toch niet per sé alle IP-adressen moeten worden aangemerkt als persoonsgegevens:

> 'Om deze reden wordt er, ook al is het wellicht niet in alle gevallen en niet voor alle internetpartijen mogelijk een gebruiker aan de hand van de op internet verwerkte gegevens te identificeren, in dit document van uitgegaan dat de mogelijkheid daartoe in veel gevallen wel degelijk bestaat en dat grote hoeveelheden persoonsgegevens waarvoor de richtlijnen op het gebied van persoonsgegevens gelden, op internet worden verwerkt.'[8]

In dezelfde periode redeneert het CBP op min-of-meer dezelfde wijze als de werkgroep – begrijpelijk omdat de toezichthouder een actief deelnemer van de werkgroep is. In 2001, in een publicatie met de veelzeggende titel 'Een IP-adres is niet altijd een persoonsgegeven' uit 2001 zet de toezichthouder uiteen wanneer en onder welke omstandigheden kan worden aangenomen dat met een IP-adres zonder onevenredige inspanningen de identiteit van een natuurlijke persoon kan worden vastgesteld.[9] De toezichthouder parafraseert de parlementaire geschiedenis die weer voortbouwt op eerdere correspondentie over dezelfde begrippen:

> 'Bij 'identified or identifiable' speelt vooral de vraag of de identiteit van de persoon redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Dit hangt mede af van de mogelijkheden waarover de houder beschikt en de bekendheid of beschikbaarheid van aanvullende informatie. Hierbij moet uitgegaan worden van een redelijk toegeruste houder. In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de houder. Het gaat dus enerzijds om objectivering naar een redelijk toegeruste houder en anderzijds om subjectivering naar bijzondere expertise.'[10]

Dit toepassend op IP-adressen komt de toezichthouder tot het oordeel dat de door een ISP uitgegeven vaste of statische IP-adressen 'zonder meer' door deze ISP zijn te herleiden tot natuurlijke personen en als persoonsgegevens moeten worden aangemerkt. Voor dynamische IP-adressen is dit anders, tenminste als de ISP niet heeft vastgelegd op welk moment het adres door welke gebruiker werd gebruikt. Het uitgangspunt is dat er geen sprake is van persoonsgegevens ten opzichte van anderen dan de ISP's, als deze anderen niet beschikken over de middelen om de internetgebruikers te identificeren.

3.2 'IP-adressen wel als zodanig behandelen' (2007)

In 2007 publiceert de werkgroep een opinie over het begrip persoonsgegevens. Voorde vraag of er sprake is van identificeerbaarheid moet, zo geeft de werkgroep aan, worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs zijn in te zetten door de verantwoordelijke zelf of iemand anders. Evenals de wetgever leidt de werkgroep daaruit af dat de theoretische of hypothetische mogelijkheid om een natuurlijke persoon te identificeren onvoldoende is om die persoon als identificeerbaar te beschouwen. Om te bepalen of sprake is van 'redelijkerwijs in te zetten middelen' moet rekening worden gehouden met alle relevante omstandigheden van het geval.
Als voorbeeld noemt de werkgroep de situatie waarin door auteursrechthebbende de IP-adressen worden verzameld van de internetgebruikers van wie wordt vermoed dat die inbreuk maken op zijn auteursrechten. In deze situatie is er volgens de werkgroep sprake van persoonsgegevens als wordt aangenomen dat de rechthebbende via gerechtelijke procedures de beschikking kan verkrijgen over daarbij behorende abonneegegevens. Maar ook dan zijn er volgens de werkgroep nog veel voorbeelden waarbij identificatie met een IP-adres onmogelijk is, zoals het geval van een internetcafé waarbij gebruiker zich niet behoeft te identificeren:

> 'In sommige gevallen is het voor bepaalde IP-adressen om diverse technische en organisatorische redenen niet mogelijk de gebruiker te identificeren. Een voorbeeld zijn de IP-adressen die zijn toegewezen aan computers in een internetcafé waar van de klanten geen legitimatie wordt verlangd. Hier zou kunnen worden aangevoerd dat de gegevens over het gebruik van computer X gedurende een bepaalde periode geen identificatie van de gebruiker met redelijkerwijs in te zetten middelen mogelijk maken en dat die gegevens daarom geen persoonsgegevens zijn.'[11]

Omdat niet in alle gevallen bekend is of er sprake is van identificeerbaarheid doet de werkgroep wel de aanbeveling dat internetdienstverleners voor de zekerheid alle IP-adressen als persoonsgegevens behandelen. Dit vooral om praktische redenen. En omdat de ISP 'naar alle waarschijnlijkheid' niet weet of het IP-adres identificatie mogelijk maakt, zal hij het IP-adres op dezelfde wijze moeten behandelen als persoonsgegevens.

3.3 'IP-adres (vrijwel) altijd een persoonsgegeven' (2007-2008)

Iets minder dan een half jaar later lijkt de werkgroep enige afstand te nemen van eerdere opvattingen over IP-adressen en persoonsgegevens. In een opinie over internetzoekdiensten kent de werkgroep niet of nauwelijks nog betekenis toe het vereiste dat moet worden gekeken naar de identificatiemiddelen waarover een verantwoordelijke redelijkerwijs de beschikking heeft. Verder ziet de werkgroep weinig ruimte

---

8. Art. 29 WG, Een geïntegreerde EU-aanpak van on-linegegevensbescherming, 21 november 2000, p. 22. < http://bit.ly/TvIR_Art29WGno37>.
9. CBP, 'Een IP adres is niet altijd een persoonsgegeven', 19 maart 2001, z2000-0340 http://bit.ly/TvIR_CBP-19maart2001.
10. Vgl. de parl. gesch, genoemd in voetnoot 3 en de brief van de Registratiekamer genoemd in voetnoot 2; in deze stukken wordt nog uitgegaan van het in de wet persoonsregistraties gebruikte begrip 'houder' in plaats van het later in de Wbp geïntroduceerde begrip 'verantwoordelijke'.
11. Art. 29 WG, Opinion nr. 4/2007 over het begrip persoonsgegevens, 20 November 2007, p. 18 <http://bit.ly/TvIR_Art29WGno136>.

meer voor de situatie waarin de éne gegevensverwerker wél identificatiemogelijkheden heeft en de andere niet:

> 'Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address.' [12]

De werkgroep komt dan tot de conclusie IP-adressen in de meeste gevallen persoonsgegevens betreffen omdat identificatie door derden mogelijk kan zijn ('identification […] by a third party'). Weliswaar kan in de regel alléén de ISP achterhalen welke natuurlijke persoon van een IP-adres gebruik heeft gemaakt. Maar omdat 'authorities' en in voorkomende gevallen zelfs 'private parties' verondersteld worden in staat te zijn om (kennelijk zonder onevenredige inspanning) van de ISP de nodige identificerende abonneegegevens te verkrijgen, meent de werkgroep dat er in de meeste gevallen ('most cases') sprake zal zijn van persoonsgegevens. De werkgroep veronderstelt aldus beschikbaarheid van de redelijkerwijs in te zetten identificatiemiddelen.
Een en ander betreft nog steeds de toepassing van de gebruikelijke, door de wetgever aangereikte criteria van 'de onevenredige inspanning' en 'de redelijkerwijs beschikbare identificatiemiddelen'. Echter, dat de werkgroep de criteria toch anders is gaan toepassen, of wellicht zelfs andere criteria is gaan toepassen, kan worden opgemaakt uit een opmerking over anonimisering *c.q.* niet-identificeerbaarheid:

> 'Anonymisation of data should exclude any possibility of individuals to be identified, even by combining anonymised information held by the search engine company with information held by another stakeholder (for instance, an internet service provider).'[13]

Volgens de werkgroep kan derhalve alleen sprake zijn van anonimisering of on-identificeerbaarheid als iedere mogelijkheid van identificering is uitgesloten ('exclude any possibility of individuals to be identified'). Of identificeren een onevenredige inspanning kost vindt de werkgroep niet meer relevant, en evenmin of het slechts om een theoretische of hypothetische mogelijkheid gaat. Dat duidt erop dat de werkgroep eigenlijk wil zeggen dat IP-adressen hoe dan ook als persoonsgegevens moeten worden aangemerkt. En dat is dan ook de conclusie die het CBP daaraan verbindt. In een persbericht over deze opinie stelt de toezichthouder zonder veel omhaal dat daarin:

> 'ondubbelzinnig [wordt] vastgesteld dat IP-adressen persoonsgegevens vormen.'[14]

Een half jaar eerder was het CBP al een stap verder gegaan. In zijn Richtsnoeren voor publicatie van persoonsgegevens op internet stelt de toezichthouder dat het niet uitmaakt of ISP's de door hen uitgegeven IP-adressen niet gebruiken om internetgebruikers te identificeren. Om IP-adressen als persoonsgegevens aan te merken is volgens de richtsnoeren voldoende dat er daartoe bij de ISP zelf, of bij anderen, de mogelijkheid bestaat. Of een onevenredige inspanning vereist of slechts een theoretische of hypothetische mogelijkheid betreft, is niet meer relevant:

> 'Een IP-adres is een persoonsgegeven omdat het door een derde – de internetaanbieder – eenvoudig te herleiden valt tot een natuurlijk persoon, de afnemer van het internetabonnement. Dit geldt ook voor dynamische IP-adressen die worden verwerkt in combinatie met datum en tijd. Het maakt geen verschil dat een verantwoordelijke het IP-adres niet zal gebruiken om een persoon mee te identificeren. Het feit dat de mogelijkheid bestaat bij de verantwoordelijke of bij een derde om dit te doen, is voldoende.'[15]

Wel onderkennen de richtsnoeren dat 'in sommige gevallen' met behulp van IP-adressen alleen rechtspersonen worden geïdentificeerd. Maar dat doet er niet aan af dat er 'in de meeste gevallen' toch wel sprake zal zijn van persoonsgegevens en er 'dus' alle gegevens hoe dan ook als zodanig moeten worden behandeld:

> 'Dat het IP-adres in sommige gevallen naar een rechtspersoon leidt, in plaats van naar een natuurlijk persoon, doet niet af aan het feit dat het in de meeste gevallen wel degelijk om persoonsgegevens gaat en dat dus de hele verzameling moet worden behandeld conform de uitgangspunten van de Wbp.'[16]

Er lijkt te zijn bedoeld dat het in deze gevallen praktisch onmogelijk is om onderscheid te maken tussen de IP-adressen die wél en niet kunnen worden gebruikt om natuurlijke personen te identificeren. Er is dan dus niet zozeer een verplichting om ook IP-adressen van rechtspersonen te behandelen alsof het persoonsgegevens zijn, maar veeleer een gemakshalve veronderstelde onvermijdelijkheid. [17]
Interessant is verder dat het CBP in zijn richtsnoeren met zoveel woorden toegeeft het eigenlijk niet meer van belang te vinden of met het IP-adres de identiteit van de internet-

12. Art. 29 WG, Opinion 1/2008 on data protection issues related to search engines, 4 April 2008 http://bit.ly/TvIR_Art-29WGno148.
13. Art. 29 WG, Opinion 1/2008 on data protection issues related to search engines, 4 April 2008 p. 20 http://bit.ly/TvIR_Art29WGno148.
14. CBP persbericht van 7 april 2008 http://bit.ly/TvIR_CBP7april2008.
15. CBP Richtsnoeren, 'Publicatie van persoonsgegevens op het internet', 11 december 2007 *Stcrt.* 2007, 240 <http://bit.ly/TvIR_CBPinternetrichtsnoeren>.
16. CBP Richtsnoeren, 'Publicatie van persoonsgegevens op het internet', 11 december 2007, p. 19 (zie ook *Stcrt.* 2007, 240) http://bit.ly/TvIR_CBPinternetrichtsnoeren.
17. In de definitieve bevindingen van een onderzoek naar de GeenStijl IP-checker volstaat het CBP overwegend met verwijzingen naar de eigen richtsnoeren. Op het verweer dat niet alle IP-adressen naar individuen verwijzen reageert het CBP met de opmerking dat het dit argument 'niet steekhoudend' acht, omdat 'het niet afdoet aan de herleidbaarheid tot een individu van een groot deel van de IP-adressen'. Ofwel: omdat een groot deel van de IP-adressen herleidbaar is tot individuen zijn alle IP-adressen persoonsgegevens. Aldus 'GeenStijl IP-checker op GeenCommentaar' 27 oktober 2008 (z2008-01174) http://bit.ly/TvIR_CBPgeenstijl.

gebruiker te achterhalen is. Wat de toezichthouder van belang vindt is dat deze internetgebruiker, hoewel niet geïdentificeerd, te maken kan krijgen met beslissingen die op basis van dat IP-adres over hem worden genomen:

> '[het] is van belang dat op basis van het IP-adres beslissingen kunnen worden genomen over de toegang tot bepaalde informatie, zonder dat een dienstverlener op internet überhaupt enige moeite hoeft te doen om zelf persoonsgegevens te verbinden aan een IP-adres. Denk bijvoorbeeld aan onderscheid naar geografische herkomst bij de toegang tot en de presentatie van (delen van) websites. Ook het registreren en eventueel op internet publiceren van IP-adressen van bezoekers van een website of deelnemers aan een discussieforum valt dus onder het bereik van de Wbp.'[18]

Als ik het goed zie doelt de toezichthouder op situaties waarin bepaalde niet-geïdentificeerde internetgebruikers op basis van een eerder door hen gebruikt IP-adressen kunnen worden geweerd van een website of niet in aanmerking komen voor een bepaalde dienst. In die situaties vindt de toezichthouder dat de verwerking van deze IP-adressen 'dus' wel onder de werkingssfeer van de Wbp valt, of zou moeten vallen, ook al is de identiteit van de internet-gebruikers niet bekend.

4. Bespreking

Uit het in de vorige paragraaf gegeven overzicht maak ik op dat de Art. 29 Werkgroep en het CBP de afgelopen jaren anders zijn gaan denken over het begrip persoonsgegevens en de vraag of IP-adressen daaronder vallen. De toezichthouders lijken steeds meer afstand te nemen van het tot dusver als algemeen als geldend recht opgevatte uitgangspunt dat IP-adressen soms wel en soms geen persoonsgegevens zijn, afhankelijk van de redelijkerwijs beschikbare identificatiemogelijkheden en de al dan niet onevenredige inspanning die is vereist om internetgebruikers te identificeren.[19] Het uitgangspunt van de toezichthouders lijkt nu te zijn dat IP-adressen eigenlijk altijd als persoonsgegevens moeten worden aangemerkt of in elk geval als zodanig moeten worden behandeld.

Een en ander is niet onbelangrijk. Een extensieve(re) interpretatie van het persoonsgegevensbegrip, zodanig dat IP-adressen vrijwel altijd daaronder vallen, betekent een verruiming van de werkingssfeer van de privacywetgeving en daarmee een uitbreiding van de reikwijdte van de bevoegdheden van privacytoezichthouders, onderwerpen die in verband met de aanstaande herziening van de richtlijn sowieso al op de agenda staan. Voldoende aanleiding dus om daarop dieper in te gaan.

Een voor de hand liggende vraag is wat de overwegingen van de toezichthouders zijn om IP-adressen onder de werking van de privacywetgeving te willen brengen. De verschillende werkdocumenten, opinies en richtsnoeren enz. zijn daarover niet erg duidelijk – in zoverre is alles wat ik daarover zeg dus enigszins speculatief. Er lijkt uit de verschillende uitlatingen van de toezichthouders wel te kunnen worden afgeleid dat deze overwegingen vooral liggen in het besef dat, als gevolg van intelligentere zoek- en profilerings-technieken,[20] IP-adressen steeds meer betekenis krijgen bij allerlei belangrijke beslissingen over individuele internetgebruikers. Aldus kan het vastleggen en gebruiken van IP-adressen, ook als er volgens de gebruikelijke maatstaven misschien nog geen sprake is van identificeerbaarheid, vergaande privacy-implicaties hebben.[21] Voor toezichthouders van wie de bevoegdheid is beperkt tot persoonsgegevens is dan de begrijpelijke eerste reflex om het persoonsgegevensbegrip zo te interpreteren dat IP-adressen (vrijwel) altijd daaronder vallen.

Voor deze overwegingen heb ik enig begrip. Er is veel voor te zeggen om internetgebruikers op de een of andere manier in staat te stellen om inzicht te hebben in, en enige zeggenschap over, de beslissingen die met gebruik van IP-adressen over hen worden genomen. Maar de benadering die de werkgroep en toezichthouders kiezen komt mij onhoudbaar voor. De wet en richtlijn gaan, niet zonder reden, uit van geïdentificeerde of identificeerbare natuurlijke personen. Er zijn talloze alledaagse voorbeelden van situaties waarin het identificeren van internetgebruikers niet meer dan een theoretische of hypothetische mogelijkheid betreft. Wat de werkgroep en het CBP daarover ook zeggen, de wet biedt geen basis om in die situaties IP-adressen zonder meer aan te merken als persoonsgegevens.

Dit wordt niet anders doordat IP-adressen worden gebruikt om beslissingen te nemen over individuele internetgebruikers, zoals het CBP stelt in zijn richtsnoeren. Wat het CBP daarmee lijkt te suggereren is dat er ook al sprake kan zijn van identificatie door alleen de gebruikte IP-adressen vast te leggen. De internetgebruiker wordt dan niet aangeduid door zijn naam, adres en andere gebruikelijke identificatiegegevens, maar alleen door middel van het IP-adres dat hij of zij op enig moment gebruikte. [22]

---

18. CBP Richtsnoeren, 'Publicatie van persoonsgegevens op het internet', 11 december 2007, p. 20 (zie ook *Stcrt.* 2007, 240) http://bit.ly/TvIR_CBPinternetrichtsnoeren.
19. In verschillende handboeken wordt ervan uitgegaan dat dit uitgangspunt als geldend recht heeft te gelden, vgl. Van Esch, *Juridische aspecten van elektronische handel*, tweede herziene druk, Deventer 2007, p. 75 en 76; zie verder bijvoorbeeld ook K. Koelman & l. Bygrave, *Privacy, Data Protection and Copyrigh,* Amsterdam 1998; T. Oudejans, 'Internet on line. Privacy off-site', *Privacy&Informatie* 1998/4, p. 153-160; R. van Esch & P. Blok, 'Privacy en elektronische handel via internet', in J.M.A. Berkvens & J.E.J. Prins. *Privacyregulering in theorie en praktijk*, Deventer 2007, p. 205-206. Een duidelijk afwijkend standpunt wordt ingenomen door H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer 2011, p. 64-65.
20. Denk in dat verband vooral aan behavorial targeting of behavorial advertizing; zie daarover J. Koeter 'Behavioral targeting en privacy: een juridische verkenning van internet gedragsmarketing', *IR* 2009, nr. 4, p. 104-111, alsmede Art. 29 WG, Advies 2/2010 over online reclame op basis van surfgedrag ('behavioural advertising'), 22 juni 2010 http://bit.ly/TvIR_Art29WGno171.
21. In die zin laat ook de Federal Trade Commission of FTC zich uit in Protecting Consumer Privacy in an Era of Rapid Change - preliminary FTC Staff Report, December 2010, p. 67 http://bit.ly/TvIR_FTC.
22. In die zin laat Hustinx, de voorzitter van de Europese privacytoezichthouder, zich uit in een kort webinterview op Zdnet: '*identifiable in the sense of personal data is signaling someone out; we don't need to name name and address*' < http://bit.ly/TvIR_Hustinx_on_IP-addresses>.

Wat het CBP aldus doet is 'identificeren' gelijkstellen aan 'individualiseren':

– individualiseren is het tegengestelde van generaliseren en betreft het kunnen aanwijzen, van anderen onderscheiden en afzonderen van een bepaalde persoon (zeg: de internetgebruiker die gebruik maakte van IP-adres 194.209.131.192);
– identificeren is het tegengestelde van anonimiseren en betreft het vaststellen wie iemand is, dus: wat zijn of haar identiteit is (zoals bijvoorbeeld de heer G-J. Zwenne uit Den Haag van wie de nawgegevens door KLM-Airfrance zijn terug te vinden via e-ticketnr. 074 2984216323 en/of FlyingBluekaartnr. KL21832-8-5585.

Het ene kan niet gelijk worden gesteld met het andere.[23] Er is discussie mogelijk over de redelijkerwijs ter beschikking staande identificatiemiddelen en de al dan niet onevenredige inspanning die is vereist om met behulp van een of meer gegevens de identiteit te achterhalen van een bepaalde natuurlijke persoon. Maar over wat 'identificeren' betekent is er denk, in elk geval binnen de kaders van de richtlijn en de wet, geen of weinig discussie mogelijk. Het komt mij voor dat de identiteit van een internetgebruiker veel meer is dan het IP-nummer waarvan hij of zij op enig moment gebruik maakte.[24]
Blijft de vraag of er, gelet op wat er allemaal kan met IP-adressen, toch niet op de een of andere manier beperkingen zouden moeten worden gesteld aan het gebruik ervan, ook als ermee nog geen natuurlijke personen kunnen worden geïdentificeerd. Ik ben geneigd deze vraag bevestigend te beantwoorden. In het tweede deel van dit tweeluik, dat in een van de volgende nummers van dit tijdschrift wordt opgenomen, kom ik daarop terug en zet ik uiteen hoe deze regulering kan worden vormgegeven.

23. Als is vastgesteld dat van de 93 passagiers slechts één de vliegtuigcrash heeft overleefd is deze daarmee geïndividualiseerd: hij is de enige overlevende en als zodanig onmiskenbaar geïndividualiseerd. Echter, om zijn familie te informeren is nodig om hem vervolgens te identificeren, d.w.z. om te achterhalen wat zijn identiteit is. Dat werd pas duidelijk toen was vastgesteld dat dit individu de negenjarige Ruben van Assouw uit Tilburg was.
24. In dit tijdschrift kwamen ook Wisman en Van der Linden Smith, bij de bespreking van vergelijkbare voorbeelden betreffende RFID- en DNA-gegevens, met enige tegenzin tot dezelfde conclusie: '*[n]aar de heersende leer vallen de genoemde voorbeelden waarschijnlijk niet onder de bescherming van de Wbp omdat de identiteit van de betrokkenen niet zonder onevenredige inspanning kan worden vastgesteld*'. Zie T. Wisman en M. van der Linden–Smith, 'My secret life as an average person', *IR*2008, nr. 4, p. 88.